

CHAPTER 6: ENFORCEMENT

6.1 Introduction

6.1.1 In a broad sense, enforcement can be understood as any action leading to better compliance with national privacy legislation, including awareness raising activities and the development of guidance. In a narrower sense, enforcement means the undertaking of investigative actions, or even solely, the imposition of sanctions.¹ In this chapter the narrower interpretation will be investigated.²

6.1.2 The grounds for starting an enforcement action in the narrow sense can vary; on the one hand, enforcement action can be based on concrete information that there is a breach of the information protection legislation. Such information can come from the complainant, from the press etc. On the other hand, oversight authorities can develop their own investigation or audit programmes. Such programs could be aimed at providing a more accurate picture of the implementation of particular information protection rules or information protection legislation within particular sectors, with a view to developing the policies of the oversight authorities, providing guidance etc. The purpose of such programs could also be to check whether or not responsible parties comply with the rules, and to aim at underlining to responsible parties what is expected of them. In investigation or audit programs, the use of formal powers, and the imposition of sanctions at a national level, could turn out to be necessary.³

6.1.3 It is therefore clear that the existence and ready availability of effective remedies against unlawful or improper processing is essential to ensure both compliance with the law generally and enjoyment of the rights and remedies of data subjects in particular.⁴

¹ EU Article 29 Data Protection Working Party **Declaration of the Article 29 Working Party on Enforcement** WP101 (12067/04/EN) Adopted on 25th November 2004 (hereafter referred to as "**WP101 on Enforcement**") at 3.

² See, however, the discussion in Chapter 5 entitled "Supervision".

³ **W101 on enforcement** at 3.

⁴ Korff **Comparative Study** at 179.

6.1.4 We have already established⁵ that the most notable difference between the self-regulatory system on the one hand and the regulatory or co-regulatory systems on the other hand, is the manner in which the information protection principles are enforced.⁶ In the self-regulatory system there is no general information protection authority to oversee the implementation of the privacy legislation. The chosen method of implementation has, on occasion, been described as “voluntary compliance and self-help” or a “dispersed responsibility method”. In other words it is up to the responsible parties themselves to comply with the Act and an individual has to enforce his or her rights under the Act through the courts.⁷ The regulatory and co-regulatory system, on the other hand, makes provision for an authority to oversee enforcement (external supervision). This is the system preferred by the Commission.

⁵ See Chapter 5 above.

⁶ See also Roos thesis at 533.

⁷ Roos thesis at 534.

6.1.5 The topic of sanctions and remedies is dealt with only in very general terms by the CoE Convention, OECD Guidelines and UN Guidelines. The EU Directive is more specific. In particular, article 28(3) states that supervisory authorities shall have investigative powers and powers to collect all the information necessary, effective powers of intervention and the power to engage in legal proceedings.⁸ Art 28(4) provides that the authority shall consider complaints.⁹ Art 22 furthermore requires that data subjects be given the right to a “judicial remedy” for “any breach” of their rights pursuant to the applicable national information protection law.¹⁰ Art 28(3) also stipulates that decisions by an information protection authority which give rise to complaints “may be appealed against through the courts”.¹¹ Finally, art 28(6) stipulates that the supervisory authorities must cooperate with one another.¹²

6.1.6 The purpose of external supervision of information protection is therefore threefold:

- * To deliver a satisfactory level of compliance with the rules contained in the information protection legislation;
- * to provide support and help to data subjects in the exercise of their rights;
- * to provide appropriate redress to prejudiced data subjects where rules are not complied with.

8

Art 28(3) provides as follows:

Each authority shall in particular be endowed with:

- * investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties.
- * effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Art 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions;
- * the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive has been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

9

Art 28(4) provides as follows:

Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

10

Article 22 provides as follows:

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

11

Art 28(3).

12

Art 28 (6) provides as follows:

Each supervisory authority..... The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

6.1.7 All information protection Acts stipulate a variety of sanctions and remedies for breach of their provisions.¹³ Provision is usually made for a combination of penalties (fines and imprisonment), compensatory damages and where applicable, revocation of licences and deregistration.

6.1.8 In the final analysis, the central question concerns the exact powers that a Commission has to order compliance with the information protection principles. Here there is a clear difference between those authorities whose powers are limited to those of investigation and recommendation, and those that can mandate changes in behaviour.¹⁴

6.2 Investigating complaints

6.2.1 All the oversight authorities are charged with investigating possible breaches of the law within their jurisdiction. As stated above, such investigations can arise out of operational activities or out of specific complaints from individual data subjects.¹⁵

6.2.2 The oversight function of information protection authorities typically encompasses the handling and resolution of complaints by citizens pertaining to the processing of personal information.¹⁶ Since few cases under information privacy laws ever reach the courts, the overwhelming majority of complaints of breach of privacy laws are resolved by Commissioners, whether by mediation or by the exercise of binding powers where they have them.¹⁷

6.2.3. In most countries the national authorities are vested with extensive powers of access to

¹³ Article 29 Working Party stated that the promotion of harmonised compliance in order to promote better compliance with data protection laws on a national level is a strategic and permanent goal of the Working Party. It has decided to exchange best practices, discuss enforcement strategies and to investigate possibilities for the preparation of EU wide, synchronised national enforcement actions for Member states.

¹⁴ Bennett and Raab *The Governance of Privacy* at 117.

¹⁵ Korff *Comparative Study* at 206.

¹⁶ Bygrave *Data Protection* at 70.

¹⁷ Greenleaf G "Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability of Asia-Pacific Privacy Commissioners" Paper originally prepared for a workshop at the International Conference of Privacy and Data Protection Commissioners, Cardiff, UK September 2002. (hereafter referred to as "Greenleaf presentation 2002") at 1. Prof Greenleaf argues the case for the publication by Commissioners of complaint resolutions.

files and filing systems used to process personal information, and the authorities can therefore usually demand full access to all relevant sites and materials.¹⁸

6.2.4 Commissioners are sometimes given astonishingly wide and strong powers of search and entry, often exercisable without a judicial warrant.¹⁹

6.2.5 After a complaint has been received the authority usually gets in touch with the responsible party concerned, “advices” and acts as a conciliator, and tries to reach an amicable solution to the dispute. In many cases, the issues are straight-forward and easily resolved on the basis of clear legal principles. For instance, a responsible party refusing to grant a data subject access to his or her information may need to be “reminded “ by the authority of its duty to allow such access. Other cases, however, are more complex, and in those the authority tries to reach a compromise acceptable to both the responsible party and the data subject. Again, this approach is almost always “successful” in the sense that the authority does not need to use formal enforcement measures: the authorities in the EU Member States have reported that they only resort to “hard” enforcement measures in a minute proportion (a few percent) of complaints.²⁰

6.2.6 Examples of the work done by Privacy Commissioners in other countries are set out in Chapter 5 above.²¹

6.2.7 In the UK the Commissioner’s 2002 Report indicated that her office received about 10,000 complaints annually, and about 5% of these (ie 500) result in “verified assessments suggesting compliance unlikely”.²²

6.3 Assessment/Audit

¹⁸ Korff *Comparative Study* at 206.

¹⁹ Korff *Comparative Study* at 200; See eg sec 34(1)(d) of the Canadian Privacy Act; sec 12(1)(d) of the Canadian PIPEDA.

²⁰ Korff *Comparative Study* at 208.

²¹ See specifically para 5.2.26 and further.

²² Greenleaf presentation 2002 at 24.

6.3.1 If a person believes processing is being carried on which directly affects him or her, he or she, or a person on his or her behalf, may apply for an assessment as to whether the processing is likely to, or unlikely to, comply with the provisions of the Act. Such an assessment may also be conducted on the initiative of the Commission itself (especially where new technology is being used for the first time).²³

6.3.2 Section 13(1)(b) of the New Zealand Act provides that when requested to do so by a responsible party (agency), the Commissioner must conduct an audit of personal information maintained by that agency for the purpose of ascertaining whether or not the information is maintained according to the information privacy principles.

6.3.3 Section 42 of the UK Data Protection Act also makes provision for this position. The Commission must, upon receipt of such a request make such an assessment, provided the Commissioner has been provided with sufficient information to identify the person making the request and the processing in question.²⁴ It furthermore stipulates the matters the Commissioner may take into account to determine the manner of the assessment. They are the extent to which the request appears to raise a matter of substance, any undue delay in making the request, and finally whether the person making the request is entitled to make a subject access request.

6.3.4 In terms of the UK legislation an information notice may be served requiring the responsible party (data controller) to furnish the Commissioner with information relating to the processing of the information. Finally special information notices may be served where requests in terms of sec 42 have been received with regard to processing for special purposes (journalism, literary and artistic purposes).

6.3.5 As is the case with enforcement notices discussed above, the latter notices are also subject to an appeal procedure set out in terms of sec 48 of the Act. Under sec 47(1) a person who fails to comply with an enforcement notice, information notice or special information notice commits an offence. A person who makes false or reckless statements in purported compliance with the notices also commits an offence.

²³ See eg section 42 of the UK Data Protection Act, 1998; section 13(1) (b) of the New Zealand Act; Sec 60 of the WBP in the Netherlands; sec 18 of the Canadian PIPEDA (private bodies); sec 37 of the Canadian Privacy Act (public bodies).

²⁴ Bainbridge *Data Protection* at 146.

6.3.6 In Canada, when an alleged breach of privacy occurs at a public body, the Office of the Information and Privacy Commission will normally assist the responsible party (agency) involved in conducting its own investigation. Since the goal in such circumstances is to seek a systemic solution, the Office depends on the investigative and auditing capacity of the public body in the first instance and then reviews the resulting report.²⁵

6.3.7 The case has therefore been argued for the use of this privacy impact assessment as an additional tool in the arsenal of the Information Commissioner.²⁶ In the last five years privacy specialists have developed an assessment model for the application of new technology or the introduction of a new service, which has good potential for raising privacy alarms at an early stage in an organisation's planning process in either the public or the private sectors.

6.3.8 The essential goal is for an organisation itself to describe personal information flows as fully as possible so that the privacy implications can be analysed and addressed in a coherent manner and compliance with fair information practices may be established. Conducting a privacy impact assessment is also an effective method of engaging a team of persons at an organisation, including technology, policy, legal and privacy specialists, to work together to identify and resolve information protection.

6.4 Advisory approach

6.4.1 In most cases, the authorities are empowered to issue legally binding (though appealable) orders. In some jurisdictions, however, the authorities either do not have such competence at all,²⁷ or they have not had it in relation to certain sectors.²⁸

6.4.2 The more advisory approach is often preferred because it avoids the adversarial relationships that arise when enforcement powers are used or threatened. It may be argued that

²⁵ Flaherty DH "How to do a Privacy and Freedom of Information Act Site Visit" A revised version of a presentation to the Privacy Laws and Business Annual Conference, Cambridge, UK, July 1998 .

²⁶ Flaherty DH "Privacy Impact Assessments: An Essential Tool for Data Protection" 2000 accessed at <http://aspe.hhs.gov/datacncl/flaherty.htm> on 15/7/2005.

²⁷ Eg Germany's Federal Data Protection Commissioner see the Federal Data Protection Act ss 24-26.

²⁸ Bygrave *Data Protection* at 71.

adverse publicity for poor privacy protection can be an effective sanction.²⁹ The implementation of the Directive does not appear to have changed the generally advisory and conciliatory approach of the national information protection authorities.³⁰

6.4.3 Even if blatant violations of the law are found (such as non-registration or processing operations) the authority will usually first only issue a “reminder”, “warning” or “advice” and it will not resort to more formal measures unless these “softer” measures are ignored or disputed.³¹ In many jurisdictions, the enforcement of information protection laws seems rarely to involve meting out penalties in the form of fines or imprisonment.

6.4.4 The authorities pride themselves on the effectiveness of their conciliatory approach, pointing out that they have to resort to hard enforcement measures in only a very limited number of cases. A variety of other means of remedying recalcitrance - most notably dialogue and, if necessary, public disclosure via the mass media - seem to be preferred instead. In other words, information protection laws often function to a relatively large extent as soft law, ie law which works by persuasion, is enforced by shame and punished by blame.³² However, the outcomes may be more in line with compromises than a solution imposed on the basis of a purely legal ruling.³³ It would appear that if the authority has a “stick behind the door” it can be more forceful in such attempts at “conciliation”.³⁴

6.4.5 The benefits of giving advice are that it gives organisations the heads-up, often early in the design phase, and before major commitment of funds, of privacy risks or roadblocks. It is furthermore pro-active and often more systemic in nature than a complaints-handling focus. There is, however, the risk that advice-giving raises the litigation risk of claim of pre-judgment, or

²⁹ Bennett and Raab *The Governance of Privacy* at 117.

³⁰ Korff *Comparative Study* at 200.

³¹ Korff *Comparative Study* at 207.

³² Bygrave *Data Protection* at 79 and references therein.

³³ Korff *Comparative Study* at 207.

³⁴ Ibid; Thus the CNIL in France has, on occasion, imposed strict conditions on processing operations which could not lawfully commence until an “opinion” has not been issued by the authority. The threat of formal action (eg the issuing of a “preliminary” enforcement notice in the UK) have been used effectively to “persuade” a data user to accept the solution “proposed” by the authority.

bias, where a complaint is later made about the matter.³⁵

6.5 Enforcement powers

6.5.1 It is often contended that the ability to negotiate with data users is facilitated by the existence of enforcement powers, even if those powers are rarely used. Moreover, government and business organisations need certainty and consistency in the application of information protection rules. The provision of a formal order-making process assures a greater level of consistency, transparency and accountability over time in the implementation of the law.³⁶

6.5.2 The Directive is silent on whether or not oversight authorities shall be able to impose fines and order compensation for damages, though such competence would clearly be compatible with the Directive. The Directive also does not specifically address whether or not these authorities must be given competence to issue legally binding orders.³⁷

6.5.3 Authorities may usually order remedial action - usually subject to an appeal to a court or a special tribunal, although often information can be blocked by the authority, or processing stopped pending such an appeal in urgent cases in which there is a serious threat to the rights and interests of individuals. In addition, in many countries, the authorities can impose administrative fines. Again, such formal actions are, in practice, used only as a very last resort.³⁸

6.5.4. The law in most countries provide for the imposition, by the national information protection authorities, of a range of formal sanctions seeking to force data users to comply with the law.³⁹

6.5.5 Examples of different enforcement procedures are as follows:

³⁵ Loukidelis D "Privacy Law Enforcement: The Experience in British Columbia Canada" Paper delivered at the APEC Symposium on Data Privacy Implementation: Developing the APEC Privacy Framework, Santiago, Chile, February 2004.

³⁶ In the UK fines may be levied on controllers (responsible parties) convicted of an offence.

³⁷ Bygrave *Data Protection* at 72. Article 28 (3) of the Directive, read in conjunction with recitals 9-11 tends to suggest that such competence is required but the wording is not entirely conclusive. Authorities are to be given "effective powers of intervention".

³⁸ Korff *Comparative Study* at 208.

³⁹ Ibid.

- a) In France, the CNIL can refuse to issue a “receipt” of a registered operation, or order changes to a processing operation on the basis of the findings of an investigation.⁴⁰
- b) The New Zealand Privacy Commissioner reaches opinions concerning breaches of the Act after investigating complaints (and also conciliates) but only the Human Rights Review Tribunal can make binding decisions.⁴¹
- c) The Australian federal Privacy Commissioner is unusual in having powers under the Privacy Act 1988 (Cth) that allow him or her both to mediate complaints, and to make “determinations” under section 52⁴² that respondents should provide various remedies, including that they should pay monetary compensation. A de novo hearing before a Court is necessary in order to enforce a determination (section 55A) but the determination is prima facie evidence of the facts on which it is based. (section 55B)⁴³
- d) In the UK the Data Protection Act 1998 gives the Commissioner powers of enforcement whilst also providing for a number of criminal offences under the Act. The Commissioner therefore has powers and functions pertaining to notification, enforcement, prosecution of offenders and powers of entry and inspection all set out in the relevant sections of the act.

A system of enforcement notices provide for three forms of notice, being:

- a) the enforcement notice;
- b) the information notice; and
- c) the special information notice.

Under section 40, if the Commissioner is satisfied that the responsible party (data controller) has contravened or is contravening any of the information protection principles, he or she may serve a notice requiring the responsible party (data controller) to take or refrain from taking specified steps within a specified time and to refrain from

⁴⁰ Ibid.

⁴¹ Greenleaf presentation 2002 at 9.

⁴² See section 52 (4) of the federal Privacy Act.

⁴³ Greenleaf presentation 2002 at 11.

processing any personal information, personal information of a specified description; or for a specified purpose or purposes or in a specified manner, after a specified time.

In deciding whether to serve a notice, any personal damage or distress caused or likely to be caused has to be taken into account. The provisions as to the service of enforcement notices are subject to restrictions as regard processing for the special purposes (journalism, literary and artistic purposes as set out in the Act).⁴⁴

The act also makes provision for the Data Protection Tribunal. The purpose of the Tribunal is primarily to hear appeals from data controllers in respect of notices served by the commissioner or determinations made by the Commissioner as to whether processing is for special purposes. A data subject, however, does not have a right to appeal to the Tribunal against a decision of the Commissioner.

6.5.6 It is important to note that the enforcement functions of the authority should always be subject to judicial overview and indeed in appropriate cases, to prior judicial authorisation (such as the issuing of a warrant). There should furthermore be safeguards in place to ensure that the law is applied both equally (with all responsible parties being treated alike) and in such a way as to fully uphold data subject rights. This means that full information on all enforcement actions of the authorities should be publicly available and that data subjects are always fully informed of the outcome of any complaints, and involved in the process. In cases of disagreement, effective and effectively available judicial remedies should be available to all interested parties.⁴⁵

6.6 Courts/judicial remedies

6.6.1 Ultimate redress in most countries is vested in the courts, and each law outlines the circumstances under which disputes might be reviewed at the judicial level.⁴⁶ Recital 55 of the EU Directive makes provision for judicial remedies.⁴⁷ Art 22 of the EU Directive⁴⁸ provides for

⁴⁴ For a discussion of information notices, see para 5.5 above.

⁴⁵ Korff *Comparative Study* at 201.

⁴⁶ Bennett and Raab *The Governance of Privacy* at 117.

⁴⁷ Recital 55 of the EU Directive which states as follows:
Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy: whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in

judicial remedies for data subjects.

6.6.2 In the EU Directive Article 24⁴⁹ permits sanctions to be imposed in case of infringement of the provisions adopted pursuant to the Directive.

6.6.3 All the EU members' laws contain extensive penal provisions, making most actions contrary to the information protection law a criminal offence, punishable by fines (or in serious aggravated case, eg where the offence was committed for gain, by imprisonment). They also allow for the possibility of criminal prosecution of company directors. They adopt somewhat different formal procedures. For instance, in the UK and Ireland criminal sanctions are largely linked to "enforcement notices" which can be issued by the information protection authorities, and which are subject to appeal,⁵⁰ while other countries rely on denunciations of wrongdoers by the national authority to the prosecuting authorities, or allow the information protection authorities themselves to bring the prosecutions. These differences reflect the different legal cultures in the Member States; they do not detract from the in-principle availability of penal sanctions in all of them.⁵¹

6.6.4 Criminal prosecutions are, however, extremely rare. In the UK the annual level of prosecutions is about 55, of which 30 have in the past been for the offence of non-registration (now not prescribed anymore). Criminal prosecutions are reserved for the most obstinate or crass law breakers such as companies which continue to maintain unregistered information bases in spite of repeated warnings, which export information in spite of such warnings or formal notices, or people who knowingly flout the law by selling confidential personal information (eg policemen who obtain access to criminal records or other confidential information on behalf of

cases where he establishes fault on the part of the data subject or in case of force majeure: whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.

48 See footnote 10 above.

49 Article 24: **Sanctions**
The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

50 Sections 40 an 48 of the UK Data Protection Act.

51 Korff **Comparative Study** at 181.

unauthorised third parties).⁵²

6.6.5 It would not be unreasonable to say that the main function of the formal sanctions is to strengthen the hand of the authority during negotiations. In some countries, most notably Spain, the information protection authorities have, however, the last few years, begun to enforce the law more strictly, by imposing very substantial fines of up to Euro 60,000.⁵³

6.6.6 In the belief that the courts are not necessarily the most suitable institutions to deal with comparatively specialised and technical issues, some countries have established small tribunals, ad hoc groups of experts that perform a quasi-judicial function.⁵⁴ In Britain, for example, the 1998 Data Protection Act establishes a Data Protection Tribunal to which individuals or data users may appeal a decision of the Information Commissioner; this body is constituted from a panel of experts as necessary. In New Zealand, an aggrieved individual may appeal a finding of the Privacy Commissioner to the Complaints Review Tribunal established under the Human Rights Commission Act of 1977.⁵⁵

6.7 Compensation

6.7.1 Article 23⁵⁶ of the EU Directive provides for compensation to the data subjects who have suffered damage.

6.7.2 All the EU Member States allow for the possibility of data subjects seeking redress, and corrective action, through the courts. This includes the possibility for data subjects to obtain

⁵² Korff *Comparative Study* at 209.

⁵³ Ibid.

⁵⁴ Bennett and Raab *The Governance of Privacy* at 118.

⁵⁵ Sec 82 of the New Zealand Privacy Act.

⁵⁶ Article 23: **Liability**

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

damages by means of court action. There are, however, differences with regard to the kinds of damages for which a claim may be lodged and the way in which provision is made for exculpatory provision specified by the Directive.⁵⁷

6.7.3 In the Netherlands the law says that the level of damages can be reduced depending on the extent to which the person being sued can be held accountable for the damage - this matter is to be determined in accordance with the ordinary rules on full or partial liability.⁵⁸

6.7.4 In the UK, too, the law provides for compensation for damage caused as a result of any failure on the part of a responsible party to comply with the law - but the law is more restrictive as concerns "distress" (ie immaterial damage) than as concerns (material) damage: the former can only be awarded if material damage has been proven. In practice, few claims are ever made.⁵⁹

6.8 Conclusion

6.8.1 It is clear that the best way of providing external supervision is through an independent oversight authority,⁶⁰ as well as by providing information subjects with legal remedies which they can enforce in a court of law.⁶¹ The oversight body should have investigative powers and powers to engage in legal proceedings where the information protection legislation has been violated. The individual should also have rights of enforcement independent of the information protection authority, such as the inherent right to approach a court or appeal to a court against a decision taken by a responsible party or the Commission itself. An individual who has suffered damage by reason of a contravention of the information protection legislation should furthermore be entitled to

⁵⁷ Korff *Comparative Study* at 180.

⁵⁸ Ibid.

⁵⁹ Korff *Comparative Study* at 180.

⁶⁰ See Chapter 5 above.

⁶¹ See discussion in Chapter 5 above; Roos thesis at 723 referring to Data Protection Working Party Transfers of personal data to third countries 4-5.

compensation by either the responsible parties or the data processors.⁶² Finally, in accordance with most other jurisdictions, the legislation should also provide for a number of criminal offences under the Act. Comment is invited.

6.8.2 The proposed legislation reads as follows:

CHAPTER 8

ENFORCEMENT

Interference with the protection of the personal information of a person -

63. *For the purposes of this Chapter, an action is an interference with the protection of the personal information of a person if, in relation to that person -*

- (i) the action breaches an information privacy principle; or*
- (ii) the provisions of section 20 of this Act have not been complied with; or*
- (iii) the provisions of section 93 of this Act have not been complied with;⁶³ or*
- (iv) the provisions of section 94 of this Act have not been complied with.*

Complaints

64. *Any person may submit a complaint to the Commission in the prescribed manner and form alleging that any action is or appears to be an interference with the protection of the personal information of a person.*

Mode of complaint to Commission

- 65. (1) *A complaint to the Commission may be made either orally or in writing.*
- (2) *A complaint made orally must be put in writing as soon as reasonably practicable.*

⁶² Summary in Roos thesis at 538.

⁶³ The New Zealand definition includes subparagraph (b) set out below. Comment is invited.

- 1.(1) For the purposes of this Part of this Act, an action is an interference with the privacy of a person if ---
- (a) In relation to that person,---
 - (i) The action breaches an information privacy principle; or
 - (ii) The provisions of Part X of this Act (which relates to information matching) have not been complied with; and
 - (b) The action has ---
 - (i) Caused, or may cause, loss, detriment, damage, or injury to that person; or
 - (ii) Adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of that person; or
 - (iii) Resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of that person.

(3) The Commission must give such reasonable assistance as is necessary in the circumstances to enable an individual, who wishes to make a complaint to the Commission, to put the complaint in writing.

Investigation by Commission

66. (1) *The functions of the Commission under this Chapter of this Act are to --*

- (a) investigate any action that is or appears to be an interference with the protection of the personal information of a person;*
- (b) act as conciliator in relation to any such action;*
- (c) take such further action as is contemplated by this Chapter of this Act.*

(2) The Commission may commence an investigation under subsection (1)(a) of this section either on complaint made to the Commission or on the Commission's own initiative.

Action on receipt of complaint

67. (1) *On receiving a complaint under this Chapter of this Act, the Commission may -*

- (a) investigate the complaint; or*
- (b) decide, in accordance with section 68 of this Act, to take no action on the complaint.*

(2) The Commission must, as soon as practicable, advise the complainant and the person to whom the complaint relates of the procedure that the Commission proposes to adopt under subsection (1) of this section.

Commission may decide to take no action on complaint

68. (1) *The Commission may in its discretion decide to take no action or, as the case may require, no further action, on any complaint if, in the Commission's opinion -*

- (a) the length of time that has elapsed between the date when the subject-matter of the complaint arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable; or*
- (b) the subject-matter of the complaint is trivial; or*
- (c) the complaint is frivolous or vexatious or is not made in good faith; or*
- (d) the person alleged to be aggrieved does not desire that action be taken or, as the case may be, continued; or*
- (e) the complainant does not have a sufficient personal interest in the subject-matter of the complaint; or*
- (f) where -*
 - (i) the complaint relates to a matter in respect of which a code of conduct issued under*

section 54 of this Act is in force; and

(ii) the code of conduct makes provision for a complaints procedure, the complainant has failed to pursue, or to pursue fully, an avenue of redress available under that complaints procedure that it would be reasonable for the complainant to pursue.

(2) Notwithstanding anything in subsection (1) of this section, the Commission may in its discretion decide not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Commission that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.

(3) In any case where the Commission decides to take no action, or no further action, on a complaint, the Commission must inform the complainant of that decision and the reasons for it.

Referral of complaint to regulatory body

69.(1) Where, on receiving a complaint under this part of the Act, the Commission considers that the complaint relates, in whole or in part, to a matter that is more properly within the jurisdiction of another regulatory body, the Commission must forthwith determine whether the complaint should be dealt with, in whole or in part, under this Act after consultation with the body concerned.

(2) If the Commission determines that the complaint should be dealt with by another body as described above, the Commission must forthwith refer the complaint to this body to be dealt with accordingly and must notify the complainant of the action that has been taken.

Pre-investigation Proceedings of Commission

70. Before proceeding to investigate any matter under this Chapter of this Act, the Commission must inform -

(a) the complainant, the person to whom the investigation relates, and any individual alleged to be aggrieved (if not the complainant), of the Commission's intention to conduct the investigation; and

(b) the person to whom the investigation relates of the ---

(i) details of the complaint or, as the case may be, the subject-matter of the investigation; and

(ii) right of that person to submit to the Commission, within a reasonable time, a written response in relation to the complaint or, as the case may be, the subject-matter of the investigation.

Settlement of complaints

71. *Where it appears from a complaint, or any written response made in relation to a complaint under section 70(b)(ii) of this Act, that it may be possible to secure a settlement between any of the parties concerned and, if appropriate, a satisfactory assurance against the repetition of any action that is the subject-matter of the complaint or the doing of further actions of a similar kind by the person concerned, the Commission may, without investigating the complaint or, as the case may be, investigating the complaint further, use his or her best endeavours to secure such a settlement and assurance.*

Investigation proceedings of the Commission

72. *For the purposes of the investigation of a complaint the Commission may -*

- (a) summon and enforce the appearance of persons before the Commission and compel them to give oral or written evidence on oath and to produce any records and things that the Commission considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record;*
- (b) administer oaths;*
- (c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commission sees fit, whether or not it is or would be admissible in a court of law;*
- (d) at any reasonable time, subject to sec 73, enter and search any premises occupied by a responsible party;*
- (e) converse in private with any person in any premises entered under section 75 subject to sec 73; and*
- (f) otherwise carry out in those premises any inquiries that the Commission sees fit in terms of sec 73.*

Issue of warrants

73. (1) *If a judge of the High Court, a regional magistrate or a magistrate is satisfied by information on oath supplied by the Commission that there are reasonable grounds for suspecting that -*

- (a) a responsible party is interfering with the protection of the personal information of a person, or*
 - (b) an offence under this Act has been or is being committed,*
- and that evidence of the contravention or of the commission of the offence is to be found on any*

premises specified in the information, it may, subject to subsection 2, provided the premises are within the jurisdiction of that judge or magistrate, grant a warrant to enter and search such premises to the Commission.

(2) A warrant issued under subsection (1) authorises the Commission or any of its officers or staff, subject to section 75, at any time within seven days of the date of the warrant to enter the premises as identified in the warrant, to search them, to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal information and to inspect and seize any record, other material or equipment found there which may be such evidence as is mentioned in that sub-section.

Requirements for issuing of warrant

74.(1) A magistrate or judge must not issue a warrant under section 73 unless he or she is satisfied-

(a) that the Commission has given seven days' notice in writing to the occupier of the premises in question demanding access to the premises, and

(b) that either-

(i) access was demanded at a reasonable hour and was unreasonably refused, or

(ii) although entry to the premises was granted, the occupier unreasonably refused to comply with a request by any of the Commission's members or officers or staff to permit the members or the officer or member of staff to do any of the things referred to in section 73(2), and

(c) that the occupier, has, after the refusal, been notified by the Commission of the application for the warrant and has had an opportunity of being heard by the judge on the question whether or not it should be issued.

(2) Subsection (1) must not apply if the judge or magistrate is satisfied that the case is one of urgency or that compliance with those provisions would defeat the object of the entry.

*(3) A judge or magistrate who issues a warrant under section 73 must also issue two copies of it and certify them clearly as copies.***Execution of warrants**

75.(1) A person executing a warrant issued under section 73 may use such reasonable force as may be necessary.

(2) A warrant issued under this section must be executed at a reasonable hour unless it appears to the person executing it that there are grounds for suspecting that the evidence in question would not be found if it were so executed.

(3) If the person who occupies the premises in respect of which a warrant is issued under

section 73 is present when the warrant is executed, he or she must be shown the warrant and supplied with a copy of it; and if that person is not present a copy of the warrant must be left in a prominent place on the premises.

(4) A person seizing anything in pursuance of a warrant under section 73 must give a receipt for it if asked to do so.

(5) Anything so seized may be retained for so long as is necessary in all the circumstances but the person in occupation of the premises in question must be given a copy of anything that is seized if he or she so requests and the person executing the warrant considers that it can be done without undue delay.

(6) A person authorised to conduct an entry and search in terms of section 73 may be accompanied and assisted by a police officer.

(7) A person who enters and searches any premises under this section must conduct the entry and search with strict regard for decency and order, and with regard for each person's right to dignity, freedom, security and privacy.

(8) A person who enters and searches premises under this section, before questioning any person -

(a) must advise that person of the right to be assisted at the time by an advocate or attorney; and

(b) allow that person to exercise that right.

Matters exempt from search and seizure

76. The powers of search and seizure conferred by a warrant issued under section 73 must not be exercisable in respect of personal information which by virtue of section 32 (exemptions) are exempt from any of the provisions of this Act.

Communication between legal adviser and client exempt

77.(1) Subject to the provisions of this section, the powers of search and seizure conferred by a warrant issued under section 73 must not be exercisable in respect of -

(a) any communication between a professional legal adviser and his client in connection with the giving of legal advice to the client with respect to his obligations, liabilities or rights under this Act, or

(b) any communication between a professional legal adviser and his client, or between such

an adviser or his client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before the court) and for the purposes of such proceedings.

(2) Subsection (1) applies also to-

(a) any copy or other record of any such communication as is there mentioned, and

(b) any document or article enclosed with or referred to in any such communication if made in connection with the giving of any advice or, as the case may be, in connection with or in contemplation of and for the purposes of such proceedings as are there mentioned.

Objection to search and seizure

78. If the person in occupation of any premises in respect of which a warrant is issued under this Schedule objects to the inspection or seizure under the warrant of any material on the ground -

- a) that it contains privileged information and refuses the inspection or removal of such article or document, the person executing the warrant or search must, if he or she is of the opinion that the article or document contains information that has a bearing on the investigation and that such information is necessary for the investigation, request the registrar of the High Court which has jurisdiction or his or her delegate, to attach and remove that article or document for safe custody until a court of law has made a ruling on the question whether the information concerned is privileged or not;*
- b) that it consists partly of matters in respect of which those powers are not exercisable, he or she must, if the person executing the warrant so requests, furnish that person with a copy of so much of the material as is not exempt from those powers.*

Return of warrants

79. A warrant issued under this section must be returned to the court from which it was issued-

(a) after being executed, or

(b) if not executed within the time authorised for its execution;

and the person by whom any such warrant is executed shall make an endorsement on it stating what powers have been exercised by him or her under the warrant **Assessment**

80. (1) The Commission, acting in its official capacity, or at a request made to the Commission by or on behalf of any person who is, or reasonably believes himself to be, affected by an action

in terms of sec 63, must make an assessment, subject to subparagraph (2), as to whether it is likely or unlikely that the processing being conducted has been or is being carried out in compliance with the provisions of this Act.

(2) The Commission must make the assessment in such manner as appears to be appropriate, unless, where the assessment is made on request, it has not been supplied with such information as it may reasonably require in order to-

(a) satisfy itself as to the identity of the person making the request, and

(b) enable it to identify the action in question.

(3) The matters to which the Commission may have regard in determining in what manner it is appropriate to make an assessment include the extent to which the request appears to it to raise a matter of substance, and where the assessment is made on request, -

(a) any undue delay in making the request, and

(b) whether or not the person making the request is entitled to make an application under Principle 7 (access) in respect of the personal information in question.

(4) Where the Commission has received a request under this section it must notify the person who made the request-

(a) whether it has made an assessment as a result of the request, and

(b) to the extent that it considers appropriate, having regard in particular to any exemption from Principle 7 applying in relation to the personal information concerned, of any view formed or action taken as a result of the request.

Information notice

81. (1) If the Commissioner-

(a) has received a request under section 80 in respect of any processing of personal information, or

(b) reasonably requires any information for the purpose of determining whether the responsible party has interfered or is interfering with the protection of the personal information of a person,

it may serve the responsible party with a notice (in this Act referred to as "an information notice") requiring the responsible party, within such time as is specified in the notice, to furnish the Commission, in such form as may be so specified, with an independent auditor's report indicating that the processing is occurring in compliance with the principles of the Act, or such information relating to the request or to compliance with the principles as is so specified.

(2) *An information notice must contain -*

(a) in a case falling within subsection (1)(a), a statement that the Commission has received a request under section 80 in relation to the specified processing, or

(b) in a case falling within subsection (1)(b), a statement that the Commission regards the specified information as relevant for the purpose of determining whether the responsible party has complied, or is complying, with the information protection principles and his reasons for regarding it as relevant for that purpose.

(3) *An information notice must also contain particulars of the rights of appeal conferred by section 85.*

(4) *Subject to subsection (5), the time specified in an information notice must not expire before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.*

(5) *If by reason of special circumstances the Commission considers that the information is required as a matter of urgency, it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion; and in that event subsection (4) must not apply, but the notice must not require the information to be furnished before the end of the period of seven days beginning with the day on which the notice is served.*

(6) *A person must not be required by virtue of this section to furnish the Commissioner with any information in respect of -*

(a) any communication between a professional legal adviser and his client in connection with the giving of legal advice to the client with respect to his obligations, liabilities or rights under this Act, or

(b) any communication between a professional legal adviser and his client, or between such an adviser or his client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before the court) and for the purposes of such proceedings.

(7) *In subsection (6) references to the client of a professional legal adviser include references to any person representing such a client.*

(8) *A person shall not be required by virtue of this section to furnish the Commissioner with any information if the furnishing of that information would, by revealing evidence of the commission of any offence other than an offence under this Act, expose him to proceedings for that offence.*

(9) *The Commissioner may cancel an information notice by written notice to the person on whom*

it was served.

(10) After completing the assessment the Commission must report to the responsible party the results of the assessment and any recommendations that the Commission considers appropriate and where appropriate a request, that within a time specified therein, notice be given to the Commission of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken.

(11) The Commission may make public any information relating to the personal information management practices of an organisation if the Commission considers it in the public interest to do so.

(12) A report made by the Commission under section 81(10) is deemed to be the equivalent to an enforcement order served in terms of sec 83 of this Act.

Parties to be informed of result of investigation

82. Where any investigation is made following a complaint, and the Commission in its discretion does not believe that an action in terms of section 63 has taken place and hence do not serve an enforcement notice, the complainant must be informed accordingly as soon as reasonably practicable after the conclusion of the investigation and in such manner as the Commission thinks proper, of the result of the investigation.

Enforcement notice

83.(1) If the Commission is satisfied that a responsible party has interfered or is interfering with the protection of the personal information of a person, the Commission may serve the responsible party with a notice (in this Act referred to as "an enforcement notice") requiring the responsible party to do either or both of the following -

- (a) to take within such time as may be specified in the notice, or to refrain from taking after such time as may be so specified, such steps as are so specified, or*
- (b) to refrain from processing any personal information, or any personal information of a description specified in the notice, or to refrain from processing them for a purpose so specified or in a manner so specified, after such time as may be so specified.*

(2) An enforcement notice must contain -

- (a) a statement indicating the nature of the interference with the protection of the personal*

information of the person and the reasons for reaching that conclusion, and

(b) particulars of the rights of appeal conferred by section 85.

(3) Subject to subsection (4), an enforcement notice must not require any of the provisions of the notice to be complied with before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

(4) If by reason of special circumstances the Commission considers that an enforcement notice should be complied with as a matter of urgency it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion; and in that event subsection (3) must not apply but the notice must not require the provisions of the notice to be complied with before the end of the period of seven days beginning with the day on which the notice is served.

Cancellation of enforcement notice

84.(1) A person on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal can be brought against that notice, apply in writing to the Commission for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the provisions of that notice need not be complied with in order to ensure compliance with the information protection principle or principles to which that notice relates.

(2) If the Commission considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with the information protection principle or principles to which it relates, it may cancel or vary the notice by written notice to the person on whom it was served.

Right of appeal

85. A person on whom an information or enforcement notice has been served may appeal to the any court of competent jurisdiction for cancellation or variation of the notice within thirty days.

Consideration of appeal

86.(1) If on an appeal under section 85 the court considers-

(a) that the notice against which the appeal is brought is not in accordance with the law,

or

(b) to the extent that the notice involved an exercise of discretion by the Commission,

that it ought to have exercised its discretion differently, the court must allow the appeal or substitute such other notice or decision as could have been served or made by the Commission; and in any other case the court must dismiss the appeal.

(2) On such an appeal, the court may review any determination of fact on which the notice in question was based.

Civil remedies

87. (1) *Either the data subject(s), or the Commission, at the request of the data subject(s), may institute civil action in any court of competent jurisdiction against any responsible party who has contravened or not complied with any provision of this Act for payment of -*

- (a) an amount determined by the Court as compensation for patrimonial and non-patrimonial damages suffered by the data subject(s) in consequence of such contravention or non-compliance;*
- (b) an amount, for compensatory or punitive purposes, in a sum determined in the discretion of the Court but not exceeding three times the amount of any profit or gain which may have accrued to the person involved as a result of any such act or omission;*
- (c) interest; and*
- (d) costs of suit on such scale as may be determined by the Court.*

(2) Any amount recovered by the Commission in terms of subsection (1) must be deposited by the Commission directly into a specially designated trust account established by the Commission with an appropriate financial institution, and thereupon-

- (a) the Commission is, as a first charge against the trust account, entitled to reimbursement of all expenses reasonably incurred in bringing proceedings under subsection (1) and in administering the distributions made to the person(s) in terms of subsection (4);*
- (b) the balance, if any (hereinafter referred to as the 'distributable balance') must be distributed by the Commission to the person(s) referred to in subsection (4), any funds remaining, accruing to the Commission in the Commission's official capacity.*

(3) Any amount not claimed within three years from the date of the first distribution of payments in terms of subsection (2), accrues to the Commission in the Commission's official capacity.

(4) The distributable balance must be distributed on a pro rata basis to the data subject(s) referred to in subsection (1): Provided that no money may be distributed to a person who has

contravened or failed to comply with any provision of this Act.

(5) A Court issuing any order under this section must order it to be published in the Gazette and by such other appropriate public media announcement as the Court considers appropriate.

(6) Any civil proceedings instituted under this section may be withdrawn, abandoned or compromised, but any agreement or compromise must be made an order of Court and the amount of any payment made in terms of any such compromise must be published in the Gazette and by such other public media announcement as the Court considers appropriate.

(7) Where civil proceedings have not been instituted, any agreement or settlement (if any) may, on application to the Court by the Commission after due notice to the other party, be made an order of Court and must be published in the Gazette and by such other public media announcement as the Court considers appropriate.

CHAPTER 9 OFFENCES AND PENALTIES

Obstruction of Commission

88. Any person who hinders, obstructs or unduly influences the Commission or any person acting on behalf or under the direction of the Commission in the performance of the Commission's duties and functions under this Act, is guilty of an offence.

Obstruction of execution of warrant

89. Any person who-

(a) intentionally obstructs a person in the execution of a warrant issued under section 73, or

(b) fails without reasonable excuse to give any person executing such a warrant such assistance as he may reasonably require for the execution of the warrant,

*is guilty of an offence.***Failure to comply with enforcement or information notices**

90.(1) A person who fails to comply with an enforcement notice served in terms of sec 83, is guilty of an offence.

- (2) A person who, in purported compliance with an information notice -
- (a) makes a statement which he knows to be false in a material respect, or
 - (b) recklessly makes a statement which is false in a material respect,
- is guilty of an offence.

Penal sanctions

91. Any person convicted of an offence in terms of this Act, is liable -
- (a) in the case of a contravention of section 88, to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and imprisonment; or
 - (b) in any other case, to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and imprisonment.

Magistrate's Court jurisdiction to impose penalties

92. Despite anything to the contrary contained in any other law, a Magistrate's Court has jurisdiction to impose any penalty provided for in section 91.

